PSI

POLÍTICA DE SEGURANÇA DA INFORMÁÇÃO

INSTITUTO FEDERAL SERGIPE

Sergipe
2011

Avenida Engº Gentil Tavares da Mota, 1166
Bairro Getúlio Vargas - Aracaju / Sergipe
CEP.: 49055-260 - CNPJ: 10.728.444/0001-00
TEL: 55 (79) 3711-3100 FAX: 55 (79) 3711-3155
www.ifs.edu.br / email: reitoria@ifs.edu.br

Instituto Federal de Educação, Ciência e Tecnologia de Sergipe

Ailton Ribeiro de Oliveira

Reitor

Pró-reitor de Desenvolvimento Institucional

Alberto Aciole Bonfim

Pró-Reitor

Diretoria de Tecnologia da Informação

Reinaldo Ferreira de Melo

Diretor

Diego Santos Cardozo

Coordenador Geral de TI

Jaziel Lobo

Coordenador de Desenvolvimento e Gerenciamento de Sistemas

André Tenório T S Silva

Coordenador de Redes

Deógenes Bispo

Coordenador de Manutenção e Suporte

Equipe de Elaboração do PSI

Adauto Menezes

André Tenório T S Silva

Diana Moura

Jadson Fábio

Reinaldo Ferreira

Acompanhamento – Equipe de Governança

Ivaniel Morais Souto

Maria do Carmo Bispo

Saulo Eduardo Galileo

Política de Segurança da Informação

1 INTRODUÇÃO

A informação é um ativo que possui grande valor para o INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE devendo ser adequadamente utilizada e protegida contra ameaças e riscos. A adoção de políticas e procedimentos que visem garantir a segurança da informação deve ser prioridade constante, reduzindo-se os riscos de falhas, os danos e/ou os prejuízos que possam comprometer a imagem e os objetivos da instituição. A informação pode existir e ser manipulada de diversas formas, ou seja, por meio de arquivos eletrônicos, mensagens eletrônicas, internet, bancos de dados, em meio impresso, verbalmente, em mídias de áudio e de vídeo etc.

Por princípio, a segurança da informação deve abranger os seguintes aspectos básicos, destacados a seguir:

(I) **Confidencialidade**: somente pessoas devidamente autorizadas pela Instituição devem ter acesso à informação.

(II) **Integridade**: somente alterações, supressões e adições autorizadas pela Instituição devem ser realizadas nas informações.

(III) **Disponibilidade**: a informação deve estar disponível para as pessoas autorizadas sempre que necessário ou demandado. Para assegurar esses três itens mencionados, a informação deve ser adequadamente gerenciada e protegida contra roubo, fraude, espionagem, perda não-intencional, acidentes e outras ameaças. A proteção da informação não é uma tarefa trivial. Em geral, o sucesso da Política de Segurança da Informação adotada por uma instituição depende da combinação de diversos elementos, dentre eles, a estrutura organizacional, as normas e os procedimentos relacionados à segurança da informação e à maneira pela qual são implantados e monitorados, os sistemas tecnológicos utilizados, os mecanismos de controle desenvolvidos, assim como o comportamento de diretores, funcionários e colaboradores.

(IV) **Autenticidade:** propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade. Atesta com exatidão a origem da informação.

2 OBJETIVO DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE é uma declaração formal acerca de seu compromisso com a proteção das informações de sua propriedade e/ou sob sua guarda, devendo ser cumprida por todos os seus colaboradores. Seu propósito é estabelecer as diretrizes a serem seguidas pelo instituto no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança da informação.

3 DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Esta Política de Segurança da Informação observa a legislação e normas específicas, destacando-se:

I. Decreto nº 7.480, de 16 de maio de 2011, que aprova a estrutura regimental e o quadro demonstrativo dos cargos em comissão do grupo-direção e assessoramento superiores – DAS e das funções gratificadas do Ministério da Educação e dispõe sobre o remanejamento de cargos em comissão.

II. Lei nº 8.112, de 11 de dezembro de 1990, que dispõe sobre o regime jurídico dos servidores públicos civis da União, das autarquias e das fundações públicas federais;

III. Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

IV. Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

V. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940. Código Penal e dá outras providências;

VI. Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil);

VII. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

VIII. Decreto nº 4.553, de 27 de dezembro de 2002, que dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal, e dá outras providências;

IX. Decreto nº 5.482, de 30 de junho de 2005, que dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores - Internet;

X. Portaria Interministerial nº 140, de 16 de março de 2006, que disciplina a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da rede mundial de computadores - internet e dá outras providências;

XI. Decreto nº 6.029, de 1º de fevereiro de 2007, que institui o Sistema de Gestão da Ética do Poder Executivo Federal, e dá outras providências;

XII. Acórdão do Tribunal de Contas da União nº 461/2004, de 28 de abril de 2004, que dispõe sobre a análise regular de arquivos logs com utilização, sempre que possível, de softwares utilitários específicos, para monitoramento do uso dos sistemas;

XIII. Instrução Normativa GSI nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências;

XIV. Norma Complementar nº 03/IN01/DSIC/GSI/PR, de 03 de julho de 2009, que estabelece as diretrizes, critérios e procedimentos para elaboração, institucionalização, divulgação e atualização da Política de Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

XV. Norma Complementar nº 04/IN01/DSIC/GSI/PR, de 17 de agosto de 2009, que estabelece diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos ou entidades da Administração Pública Federal, direta e indireta - APF;

XVI. Norma Complementar nº 05/IN01/DSIC/GSI/PR, de 17 de agosto de 2009, que disciplina a criação de Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração

Pública Federal, direta e indireta - APF;

XVII. Norma Complementar nº 06/IN01/DSIC/GSI/PR, de 23 de novembro de 2009, que disciplina as Diretrizes para Gestão de Continuidade de Negócios nos aspectos relacionados à Segurança da Informação e Comunicações - GCN nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

XVIII. Norma Complementar nº 07/IN01/DSIC/GSI/PR, de 07 de maio de 2010, que disciplina as diretrizes para implementação de Controles de Acesso relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal, direta e indireta - APF;

XIX. Norma Complementar nº 08/IN01/DSIC/GSI/PR, de 24 de agosto de 2010, que disciplina o gerenciamento de Incidentes de Segurança em Redes de Computadores realizado pelas Equipes de Tratamento e Resposta a Incidentes de Segurança em Redes Computacionais - ETIR dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XX. Norma Complementar nº 09/IN01/DSIC/GSIPR, que estabelece orientações específicas para o uso de recursos criptográficos como ferramenta de controle de acesso em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal, direta e indireta;

XXI. Norma Complementar nº 10/IN01/DSIC/GSIPR, que estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;

XXII. Norma Complementar nº 11/IN01/DSIC/GSIPR, Estabelece diretrizes para avaliação de conformidade nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos ou entidades da Administração Pública Federal, direta e indireta – APF;

XXIII. Norma Complementar nº 12/IN01/DSIC/GSIPR, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

XXIV. Norma Complementar nº 13/IN01/DSIC/GSIPR, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da

Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF);

XXV. Norma Complementar nº 14/IN01/DSIC/GSIPR, Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;

XXVI. Norma ABNT NBR ISO/IEC 27001:2006 – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos;

XXVII. Norma ABNT NBR ISO/IEC 27002:2005 – Técnicas de segurança - Código de práticas para a segurança da informação;

XXVIII. Norma ABNT NBR ISO/IEC 27005:2008 - Técnicas de segurança - Gestão de riscos de segurança da informação; e

XXIX. E-PING – Padrões de interoperabilidade de Governo Eletrônico, de 16 de dezembro de 2008.

4 ESTRUTURA DA SEGURANÇA DA INFORMAÇÃO

4.1 DEFINIÇÕES

Na presente Política, os seguintes termos deverão ser observados com as respectivas conceituações:

I - Segurança da Informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

II - Gestão de Segurança da Informação e Comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, à tecnologia da informação e comunicações;

III - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

IV - tratamento da informação: recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação, inclusive as sigilosas.

4.2 ESTRUTURA ORGANIZACIONAL

A estrutura organizacional da Segurança da Informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

Nível 1: Reitoria - autoridade máxima responsável pelo Instituto;

Nível 2: Comitê Gestor de Segurança da Informação – constituído no mínimo pelos seguintes membros:

- O titular da Reitoria;
- Um representante de cada pró-reitoria;
- O titular da Diretoria de Tecnologia da Informação;
- O titular da Área de Gestão de Segurança da Informação;
- Um representante de cada coordenação da Diretoria de Tecnologia da Informação
- Um representante da área de TI de cada campus deste Instituto.

Nível 3: **Área de Gestão de Segurança da Informação -** área funcional ligada hierarquicamente à Diretoria de Tecnologia da Informação ou a Reitoria diretamente à Reitoria.

4.3 CATEGORIAS NORMATIVAS

A estrutura normativa da Segurança da Informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE é composta por um conjunto de documentos com três níveis hierárquicos distintos, relacionados a seguir:

- **Política de Segurança da Informação (Política)**: constituída neste documento, define a estrutura, as diretrizes e as obrigações referentes à segurança da informação, e será detalhada em documentos denominados

Normas;

- **Normas de Segurança da Informação (Normas)**: estabelecem obrigações e procedimentos definidos de acordo com as diretrizes da Política, a serem seguidos em diversas situações em que a informação é tratada. A cada Norma será associado um conjunto de Procedimentos destinados a orientar sua implementação. A elaboração das Normas seguirá as orientações contidas em um documento do Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República intitulado Atividade de Normatização;
- **Procedimentos de Segurança da Informação (Procedimentos)**: instrumentalizam o disposto nas Normas e na Política, permitindo a direta aplicação nas atividades do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, cabendo a cada gestor a responsabilidade de gerá-los. Cada procedimento poderá ainda ser detalhado em instruções. Estes procedimentos e instruções são de uso interno, não sendo obrigatória a sua publicação.

4.4 DIVULGAÇÃO E ACESSO À ESTRUTURA NORMATIVA

A Política e as Normas de Segurança da Informação devem ser divulgadas a todos os colaboradores do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE e dispostas de maneira que seu conteúdo possa ser consultado a qualquer momento. Os Procedimentos de Segurança da Informação devem ser divulgados às áreas diretamente relacionadas à sua aplicação.

3.5 APROVAÇÃO E REVISÃO

Os documentos integrantes da estrutura normativa da Segurança da Informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE deverão ser aprovados e revisados conforme os seguintes critérios:

- **Política:**

  Nível de Aprovação: Reitoria;

Periodicidade de Revisão: anual.

- **Normas:**

  Nível de Aprovação: Comitê Gestor de Segurança da Informação;

  Periodicidade de Revisão: anual.

- **Procedimentos:**

  Nível de Aprovação: Diretoria responsável pela área envolvida;

  Periodicidade de Revisão: anual.

5 ATRIBUIÇÕES E RESPONSABILIDADES NA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Cabe a todos os colaboradores (funcionários, estagiários e prestadores de serviços) do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE;
- Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança da informação;
- Assinar Termo de Responsabilidade, formalizando a ciência e o aceite da Política e das Normas de Segurança da Informação, bem como assumindo responsabilidade por seu cumprimento;
- Proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados pelo INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE;
- Assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pelo INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE;
- Cumprir as leis e as normas que regulamentam os aspectos de propriedade intelectual;
- Comunicar imediatamente à área de Gestão de Segurança da Informação qualquer descumprimento ou violação desta Política e/ou de suas Normas e Procedimentos.

4.1 REITORIA

Em relação à segurança da informação, cabe à Reitoria:

- Aprovar a Política de Segurança da Informação e suas revisões;
- Aprovar a nomeação dos "proprietários" da informação;
- Tomar as decisões administrativas referentes aos casos de descumprimento da Política e/ou de suas Normas encaminhados pelo Comitê Gestor de Segurança da Informação;
- Informar, prontamente, à área gestora de segurança da informação, sobre as mudanças na estrutura organizacional (organograma) deste Instituto.

5.2 COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO (CGSI)

Cabe ao Comitê Gestor de Segurança da Informação, além das atribuições conferidas pelo artigo 6º (sétimo) da Instrução Normativa n° 01 de 13 de junho de 2008, expedida pelo GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA:

- Propor ajustes, aprimoramentos e modificações desta Política;
- Propor melhorias e aprovar as Normas de Segurança da Informação;
- Definir a classificação das informações pertencentes ou sob a guarda do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, com base no inventário de informações apresentado pela Área de Gestão de Segurança da Informação e nos critérios de classificação constantes de Norma específica;
- Analisar os casos de violação desta Política e das Normas de Segurança da Informação, encaminhando-os à Diretoria Executiva, quando for o caso;
- Propor projetos e iniciativas relacionados à melhoria da segurança da informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE;
- Propor o planejamento e a alocação de recursos financeiros, humanos e de tecnologia, no que tange à segurança da informação;
- Determinar a elaboração de relatórios, levantamentos e análises que dêem suporte à gestão de segurança da informação e à tomada de decisão;

- Acompanhar o andamento dos principais projetos e iniciativas relacionados à segurança da informação;
- Propor a relação de "proprietários" das informações do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE.

O Comitê de Auditoria do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE poderá, caso queira, indicar representante para participar das reuniões do CGSI na condição de observador/ouvinte. A coordenação dos trabalhos do CGSI caberá ao responsável pela área de Gestão de Segurança da Informação, cujas atribuições abrangerão a convocação das reuniões e a realização de outros atos de suporte às atividades desenvolvidas.

4.2.1 Das reuniões do CGSI:

- As reuniões do CGSI serão realizadas mensalmente, podendo haver convocação em frequência maior ou extraordinariamente, sempre que necessário. Serão instaladas com a presença de, no mínimo, 2/3 (dois terços) dos membros do CGSI e deverão ser registradas em ata;
- O CGSI deliberará por maioria dos votos presentes;
- De acordo com a necessidade, outros profissionais do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE e convidados externos poderão participar das reuniões do CGSI.

4.3 ÁREA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO (AGSI)

Cabe à área de Gestão de Segurança da Informação, além das atribuições conferidas pelo artigo 7º (sétimo) da Instrução Normativa n° 01 de 13 de junho de 2008, expedida pelo GABINETE DE SEGURANÇA INSTITUCIONAL DA PRESIDÊNCIA DA REPÚBLICA:

- Convocar, coordenar, lavrar atas e prover apoio às reuniões do CGSI;
- Prover todas as informações de gestão de segurança da informação solicitadas pelo CGSI;

- Prover ampla divulgação da Política e das Normas de Segurança da Informação para todos os colaboradores do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE;
- Oferecer orientação e treinamento sobre a Política de Segurança da Informação e suas Normas a todos os colaboradores do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE;
- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, mantendo-se atualizada em relação às melhores práticas existentes no mercado e em relação às tecnologias disponíveis;
- Estabelecer procedimentos e realizar a gestão dos sistemas de controle de acesso do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, incluindo os processos de concessão, manutenção, revisão e suspensão de acessos aos usuários;
- Analisar os riscos relacionados à segurança da informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE e apresentar relatórios periódicos sobre tais riscos ao CGSI, acompanhados de proposta de aperfeiçoamento do ambiente de controle do instituto, quando for o caso;
- Realizar trabalhos de análise de vulnerabilidade, com o intuito de aferir o nível de segurança dos sistemas de informação e dos demais ambientes em que circulam as informações do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE;
- Requisitar informações às demais áreas do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE (diretorias, gerências coordenações etc.), realizar testes e averiguações em sistemas e equipamentos, com o intuito de verificar o cumprimento da Política e das Normas de Segurança da Informação;
- Estabelecer mecanismo de registro e controle de não-conformidade a esta Política e às Normas de Segurança da Informação, comunicando o CGSI.

4.4 PROPRIETÁRIO DA INFORMAÇÃO

O proprietário da informação é um diretor ou um gerente do INSTITUTO

FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, formalmente indicado pela Reitoria, responsável pela concessão, manutenção, revisão e cancelamento de autorizações de acesso a determinado conjunto de informações pertencentes à instituição ou sob a sua guarda.

Cabe ao proprietário da informação:

- Elaborar, para toda informação sob sua responsabilidade, matriz que relaciona cargos e funções do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE às autorizações de acesso concedidas;
- Autorizar a liberação de acesso à informação sob sua responsabilidade, observadas a matriz de cargos e funções, a Política e as Normas de Segurança da Informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE;
- Manter registro e controle atualizados de todas as liberações de acesso concedidas, determinando, sempre que necessário, a pronta suspensão ou alteração de tais liberações;
- Reavaliar, sempre que necessário, as liberações de acesso concedidas, cancelando aquelas que não forem mais necessárias;
- Analisar os relatórios de controle de acesso fornecidos pela área de Gestão de Segurança da Informação, com o objetivo de identificar desvios em relação à Política e às Normas de Segurança da Informação, tomando as ações corretivas necessárias;
- Participar da investigação de incidentes de segurança relacionados à informação sob sua responsabilidade;
- Participar, sempre que convocado, das reuniões do Comitê de Gestão de Segurança da Informação, prestando os esclarecimentos solicitados.

4.5. JURÍDICO

Cabe ao Jurídico:

- Manter as áreas do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE informadas sobre eventuais alterações legais

e/ou regulatórias que impliquem responsabilidade e/ou ações envolvendo a gestão de segurança da informação;

- Incluir, na análise e na elaboração de contratos, sempre que necessário, cláusulas específicas relacionadas à segurança da informação, com o objetivo de proteger os interesses do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE;
- Avaliar, quando solicitada, as Normas e os Procedimentos de Segurança da Informação elaborados pelas diversas áreas do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE.

4.6 DIRETORIAS, GERÊNCIAS E COORDENAÇÕES

Cabe às Diretorias, Gerências e Coordenações:

- Cumprir e fazer cumprir esta Política, as Normas e os Procedimentos de Segurança da Informação;
- Assegurar que suas equipes possuam acesso e conhecimento desta
- Política, das Normas e dos Procedimentos de Segurança da Informação;
- Redigir os Procedimentos de Segurança da Informação relacionados às suas áreas, mantendo-os atualizados;
- Comunicar imediatamente eventuais casos de quebra de segurança à área de Gestão de Segurança da Informação.

4.7 ÁREA DE RECURSOS HUMANOS

Cabe à área de Recursos Humanos:

- Colher a assinatura do Termo de Responsabilidade por uso dos Recursos de Tecnologia da informação dos funcionários e estagiários, arquivando-o nos respectivos prontuários;
- Informar, prontamente, à área de Gestão de Segurança da Informação, da admissão e dos desligamentos e afastamentos, assim como quaisquer modificações no quadro funcional do Instituto.

5 DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

A seguir, são apresentadas as diretrizes da Política de Segurança da Informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE. Tais diretrizes constituem os principais pilares da Gestão de Segurança da Informação do instituto, norteando a elaboração das Normas e dos Procedimentos.

5.1 ADOÇÃO DE COMPORTAMENTO SEGURO

Independentemente do meio ou da forma em que exista, a informação está presente no trabalho de todos os profissionais. Portanto, é fundamental para a proteção e salvaguarda das informações que os profissionais adotem comportamento seguro e consistente com o objetivo de proteção das informações do instituto, com destaque para os seguintes itens:

- Diretores, coordenadores, servidores e prestadores de serviços devem assumir atitude pró-ativa e engajada no que diz respeito à proteção das informações do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE.
- Os colaboradores do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE devem compreender as ameaças externas que podem afetar a segurança das informações do Instituto, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de informação.
- Todo tipo de acesso à informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE que não for explicitamente autorizado é proibido.
- Informações confidenciais do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE não podem ser transportadas em qualquer meio (CD, DVD, disquete, pen-drive, papel etc.) sem as devidas autorizações e proteções.
- Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontros sociais etc.).

- As senhas de usuário são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros (inclusive colaboradores do próprio instituto), anotadas em papel ou em sistema visível ou de acesso não-protegido.
- Somente softwares homologados pelo INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE podem ser instalados nas estações de trabalho, o que deve ser feito, com exclusividade, pela equipe de serviços de informática do instituto.
- A política para uso de internet e correio eletrônico deve ser rigorosamente seguida. Arquivos de origem desconhecida nunca devem ser abertos e/ou executados.
- Documentos impressos e arquivos contendo informações confidenciais devem ser adequadamente armazenados e protegidos.
- Qualquer tipo de dúvida sobre a Política de Segurança da Informação e suas Normas deve ser imediatamente esclarecido com a área de Gestão de Segurança da Informação.

5.2 ADOÇÃO DE INVENTÁRIO E DE SISTEMA DE CLASSIFICAÇÃO DA INFORMAÇÃO

A área de Gestão de Segurança da Informação deve manter um inventário atualizado que identifique e documente a existência e as principais características de todos os seus ativos de informação (base de dados, arquivos, diretórios de rede, trilhas de auditoria, códigos fonte de sistemas, documentação de sistemas, manuais, planos de continuidade etc.).

As informações inventariadas devem ser classificadas de acordo com o grau de confidencialidade e criticidade para o negócio do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, e com base na Norma de classificação de informações estabelecida pelo instituto. As informações inventariadas devem ser associadas a um "proprietário", formalmente designado pela Reitoria como responsável pela autorização de acesso às informações sob a sua responsabilidade.

5.3 AVALIAÇÃO CONTÍNUA DOS RISCOS DE SEGURANÇA DA

INFORMAÇÃO

A área de Gestão de Segurança da Informação deve realizar, de forma sistemática, a avaliação dos riscos relacionados à segurança da informação do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE.

A análise dos riscos deve atuar como ferramenta de orientação ao Comitê Gestor da Segurança da Informação, principalmente, no que diz respeito à:

- Identificação dos principais riscos aos quais a informação do instituto está exposta;
- Priorização das ações voltadas à mitigação dos riscos apontados, tais como implantação de novos controles, criação de novas regras e procedimentos, reformulação de sistemas etc. O escopo da análise/avaliação de riscos de segurança da informação pode ser toda a organização, partes da organização, um sistema de informação específico, componentes de um sistema específico etc.

5.4 GESTÃO DE ACESSO A SISTEMAS DE INFORMAÇÃO E A OUTROS AMBIENTES LÓGICOS

Todo acesso às informações e aos ambientes lógicos do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE deve ser controlado, de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação. A política de controle de acesso deve ser documentada e formalizada por meio de Normas e Procedimentos que contemplem, pelo menos, os seguintes itens:

- Procedimento formal de concessão e cancelamento de autorização de acesso a usuário aos sistemas de informação;
- Comprovação da autorização do proprietário da informação;
- Utilização de identificadores de usuário (ID de usuário) individualizados, de forma a assegurar a responsabilidade de cada usuário por suas ações;
- Verificação se o nível de acesso concedido é apropriado ao propósito do

negócio e se é consistente com a Política de Segurança da Informação e suas Normas;

- Remoção imediata de autorizações dadas a usuários afastados ou desligados do instituto, ou que tenham mudado de função;
- Processo de revisão periódica das autorizações concedidas;
- Política de atribuição, manutenção e uso de senhas.

5.5 MONITORAÇÃO E CONTROLE

Os sistemas, as informações e os serviços utilizados pelos usuários são de exclusiva propriedade do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE, não podendo ser interpretados como de uso pessoal.

Todos os profissionais e colaboradores do INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA DE SERGIPE devem ter ciência de que o uso das informações e dos sistemas de informação da do instituto pode ser monitorado, e que os registros assim obtidos poderão ser utilizados para detecção de violações da Política e das Normas de Segurança da Informação e, conforme o caso, servir como evidência em processos administrativos e/ou legais.

6 VIOLAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SANÇÕES

Nos casos em que houver violação desta Política ou das Normas de Segurança da Informação, resultando em quebra da segurança, sanções administrativas e/ou legais poderão ser adotadas, podendo culminar com eventuais processos administrativos, se aplicáveis.